



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,904	06/28/2001	Yves Louis Gabriel Audebert	L741.01105	1582

7590 01/29/2007
STEVENS, DAVIS, MILLER & MOSHER, LLP
Suite 850
1615 L Street, N.W.
Washington, DC 20036

EXAMINER

SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
----------	--------------

2136

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)
	09/892,904	AUDEBERT ET AL.
	Examiner Eleni A. Shiferaw	Art Unit 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 14 November 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 62-73, 86, 90, 92, 94 and 95 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) 86 and 94 is/are allowed.
- 6) Claim(s) 62-63, 67, 71-73, 90, 92, and 95 is/are rejected.
- 7) Claim(s) 64-66 and 68-70 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office Action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)	5) <input type="checkbox"/> Notice of Informal Patent Application
Paper No(s)/Mail Date _____	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. Applicant's election with traverse of 62-73, 86, 90, 92, 94 and 95 in the reply filed on 11/14/2006 is acknowledged. The traversal is on the ground(s) that no unduly extensive or burdensome search would be required to examine the various claims of the noted groups in the same application. This is not found persuasive because an application should relate to only **one invention and also it does create search burden for the office**. Invention I and II are unrelated. Inventions are unrelated if it can be shown that they are not disclosed as capable of use together and they have different modes of operation, different functions, or different effects (MPEP § 808.01).

The requirement is still deemed proper and is therefore made FINAL.

Response to Amendment/Argument

2. Applicant cancels all claims and rewrites claims 62-73, 86, 90, 92, 94 and 95 and leave claims 74-85, 87-89, 91, 93-93, and 96-97 non-elected with traverse. Argument is moot in new ground of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Art Unit: 2136

4. Claims 62-63, 67, 71-73, and 90 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al. USPN 5,396,558 in view of Takahashi et al. 2000-338868 and Davis USPN 5,473,692.

Regarding claims 62 and 90, Ishiguro et al. discloses a data processing system for generating a key protection certificate comprising:

a Personal Security Device (PSD) (fig. 1 element 6; *IC card*) comprising a unique device name (fig. 5A element 6M; *IDU... card identification*), a cryptography section (col. 20 lines 26-31 and col. 19 lines 2-9), a data processing section (fig. 5A), a data storage section (fig. 3 element 64, 61, and 62) and a communications section (fig. 3 element 65), wherein said cryptography section, a first securely shared secret key (fig. 5 elements pU, qU, and nA), a symmetric cryptography section (fig. 6 element 6M1), a concatenation algorithm (col. 10 lines 12-24; *IC card concatenating V, SA(V*IDU) and digital signature of IC card using concatenation algo.*), a message authentication code algorithm (col. 9 lines 21-23 and fig. 5A element 6A), cryptographic seed information (fig. 5A element 6C), and a key protection certificate generating algorithm (fig. 5A element 6B; *signature algorithm*), and wherein said key protection certificate generating algorithm produces conditionally, upon completion by said PSD of said asymmetric cryptographic key pair generation and in dependence on said generated asymmetric cryptographic key pair, a unique digital certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair (col. 8 lines 40-44 and col. 10 lines 13-24; *signature algorithm generating a unique digital signature to R, V, and X using pU and qU*).

Ishiguro et al. fails to disclose wherein said key protection certificate generating algorithm produces conditionally with said asymmetric cryptographic key pair, a unique digital certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD.

Takahashi et al. discloses key protection certificate generating algorithm produces conditionally with said asymmetric cryptographic key pair, a unique digital certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD (par. 0011-0017).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Takahashi et al. within the system of Ishiguro et al. because they are analogous in signature generation and authentication. One would have been motivated to incorporate the teachings of Takahashi et al. with in the system of Ishiguro et al. because it would authenticate the integrate the key of the integrated card/PID.

Ishiguro et al. and Takahashi et al. fail to teach the cryptographic key pair generation algorithm of the PID.

Davis discloses an IC card comprising a public/private key generation algorithm to generate public/private key (see abstract) that reads on wherein said cryptography section includes an asymmetric cryptographic key pair generating algorithm.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Davis within the combination system because they are analogous in IC card data security. One would have been motivated to do so because it would be secure to generate the keys inside the card and not letting other device

know the keys when generated.

Regarding claim 63 the combination discloses the system, wherein at least a portion of said cryptographic seed information is used by said asymmetric key pair generating algorithm to generate at least one asymmetric private key and one asymmetric public key upon receipt of at least one key generation command (Davis abstract; *random number for pub/private key generation*), said keys being stored in a secure domain of said PSD (Ishiguro et al. fig. 6 element 6M1). The rational for combining are the same as claim 62 above.

Regarding claim 67, Ishiguro et al. discloses the system, wherein a signed device name is generated using said unique device name and said asymmetric private key as inputs into said *signing* algorithm (fig. 6 *SA(nU*IDU)*).

Regarding claim 71, Ishiguro et al. discloses the system, wherein said unique device name is an embedded serial number (col. 2 lines 66-67).

Regarding claim 72 Ishiguro et al. discloses the system, wherein said unique device name is the result of a cryptographic process using said embedded serial number as a cryptographic seed (col. 3 lines 35-45).

Regarding claim 73, the combination teaches the system, wherein said communications section (Ishiguro et al. fig. 3 element 64) includes a receiving section that receives commands to generate asymmetric and symmetric keys (Davis claim 1, and col. 5 lines 32-45) and a

sending section that sends said public key (Ishiguro et al. fig. 6 sending nU) and said key protection certificate (Takahashi et al. par. 0018-0020; *key certificate*). The rational for combining are the same as claim 62 above.

5. Claims 92 and 95 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis USPN 5,970,147 in view of Takahashi et al. 2000-338868.

Regarding claims 92 and 95 Davis discloses a method for generating a key protection certificate comprising sending a command to a personal security device (PSD) (col. 3 lines 33-45; *smart card*) comprising a unique device name (col. 2 lines 1-2) and a first securely shared secret key (col. 2 lines 40-53, and col. 4 lines 40-54) for generating at least one asymmetric cryptographic key pair (abstract), wherein said command initiates generation by said PSD of said asymmetric cryptographic key pair (claim 1).

Davis fails to explicitly disclose the key protection certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD. However Takahashi et al. discloses the key protection certificate that comprises a proof of possession by said PSD of said first securely shared secret key and of said asymmetric cryptographic key pair generated by said PSD (par. 0011-0017). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Takahashi et al. within the system of Davis because they are analogous in signature generation and authentication. One would have been motivated to incorporate the teachings of Takahashi et al. with in the system of Davis

because it would authenticate the integrate the key of the integrated card/PID.

• ***Allowable Subject Matter***

6. Claim 86 and 94 are allowed. Claims 62, 90 and 92 would be allowable if rewritten to include all the limitation of 86 and/or rewritten to include dependent claims 64-66 and 68-70.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

28

January 22, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/23/07